SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

REMOTE AUTHENTICATION CACHING ON A TRUSTED CLIENT OR GATEWAY SYSTEM

Background of Invention

[0001] As computer networks proliferate and the use of the internet, intranets and other remote methods of providing computer resources and services become more popular, the problem of authenticating users becomes more and more important. It is imperative for providers of resources such as banking services, databases holding personal or other sensitive information and internal company resources, for example, to be able to reliably identify users attempting to access their resources. As such, well known standards and methods have been developed to provide for user authentication. Many such standards and methods involve the remote exchange of some type of user authentication credential.

[0002] A user attempting to access a secure resource might be asked to enter some identifying information, such as a user id and/or a password. Behind the scenes and transparent to the user, the user's system would send the identifying information to an authentication server connected to the user's system via a network, such as the internet. Assuming the authentication server recognizes the identifying information as associated with an authorized user, an authenticated credential would be returned to the user's system, with which the user would be allowed to access the requested resource. The nature of the identifying information and the methods used by the user's system and the authentication server to verify the user's right to access the resource can all be in accordance with any one of the well-known standards regarding such functions. These methods and standards are easily identified by those skilled in the relevant arts.

[0003] One popular standard that has been developed for remote authentication of users is the Light-weight Directory Access Protocol (LDAP). LDAP may be used to authenticate users to access resources that may reside locally or remotely to the user. Typically, especially in small business environments, the LDAP server is located remotely from the user. Utilizing a remote LDAP server provided through a service provider allows the small business to save the cost of providing its own local LDAP servers. Connectivity to the LDAP server is provided via the internet, an intranet or other computer network. Figure 1 shows one possible LDAP configuration. The user's system (or client) 10 is located on a local area network (LAN) 20 to which resources 30 are also connected. These resources can include various media such as databases or world-wide web content or computer-implemented services such as banking services, training courseware, etc. Some of these resources 30 may be secure resources, the use of which requires user authentication. The client 10 is also connected to a computer network 40, such as the internet or an intranet, via a secure gateway machine 50. The gateway machine 50 may provide connectivity to the network for other clients (not shown) as well. The presence of the gateway 50 is optional as the client 10 may be connected directly to the computer network 40. Also connected to the network 40 is an LDAP server 60 for providing LDAP user authentication services for the client 10 and other systems utilizing its services (not shown) and other secure resources (30) which may be accessed by the client 10.

[0004] In order to access resources 30 which require user authentication, the client 10 must contact the LDAP server 60 and receive an authenticated credential. When the LDAP server is unavailable, such as when any of the connections between the client and the LDAP server are down (i.e., the client-gateway connection, the gateway-network connection or the network-LDAP server connection) or when the LDAP server or the gateway machine is down, user authentication is not possible and the user is unable to access the desired secure resource(s). In the case of a business environment, this can cause serious productivity losses.

[0005] In some instances, some resources 30 may be located on the client machine 10. Authentication of the user by the LDAP server 60 would still be required before the user could access such resources. In the case where the client 10 is a mobile computer, the client will often be disconnected from the network. In such an instance,

the user would be unable to access the secure resources on the mobile client because there would be no connectivity to the LDAP server. Again, serious productivity losses could result.

[0006] For these reasons, and others readily identified by those skilled in the art, it would be desirable to develop techniques to allow user's some access rights to secure resources when a remote authentication server is unavailable while maintaining a high degree of trust.

Summary of Invention

[0007] The present invention contemplates a method whereby a user may access secure resources requiring user authentication when the remote authentication server is unavailable. This method is applicable to any user authentication method or standard requiring an exchange with a remote server of some type of credential. The present invention does not require any changes to the user authentication method or standard. In realizing these and other purposes of the present invention, a method calls for a client machine to locally store the authenticated credential received from the authentication server during a successful user authentication. The credential is stored in a manner that makes tampering or falsifying the authenticated credential difficult or impossible. One example of a method of protecting the credential is hardware-based Public Key Infrastructure, or PKI, but any other appropriate method may be used. Where the client machine is connected to the authentication server via a secure gateway machine, the credential may also be stored in a similarly-secured manner on the gateway machine. Then, if a later requested user authentication fails due to a lack of availability of the authentication server, the authenticated credential on the client machine and/or the gateway machine can be used to allow the user access to the secure resource. Access to secure resources using a locally-stored credential may be limited by system policies limiting the amount of time since the last remote server authentication or other policies ensuring the security of the resource. Also, some especially sensitive resources may have associated policies that are more demanding, accepting only credentials from the gateway machine or the remote server itself.

Brief Description of Drawings

[0008] Some of the purposes of the invention having been stated, others will appear as the description proceeds, when taken in conjunction with the accompanying drawing, in which:

[0009] *Figure 1* is a block diagram showing one system configuration to which the present invention may be applied.

[0010] *Figure 2* is a flow-chart illustration of a system operating according to the present invention.

[0011] *Figure 3* is a flow chart illustration of another embodiment of a system operating according to the present invention.

Detailed Description

[0012] While the present invention will be described more fully hereinafter with reference to the accompanying drawings, in which a preferred embodiment(s) of the present invention is shown, it is to be understood at the outset of the description which follows that persons of skill in the appropriate arts may modify the invention here described while still achieving the favorable results of the invention. Accordingly, the description which follows is to be understood as being a broad, teaching disclosure directed to persons of skill in the appropriate arts, and not as limiting upon the present invention.

[0013] Devices and systems implementing the LDAP standard method of remote authentication, and other remote authentication mechanisms to which the present invention may be applied, are well known to persons skilled in the relevant arts. Such devices and systems may be implemented in any of the many alternate embodiments that are available without departing from the spirit of the present invention. Detailed descriptions of such devices and systems, and the underlying remote authentication mechanisms, are not required for an understanding of the present invention. This invention relates to an improvement to the method of operation of such devices and systems.

[0014] The figures and examples given in this description often reference the LDAP remote authentication standard and include an LDAP server as a component. The use

of these specific examples is not to be read as limiting on the present invention in any way and is simply illustrative of one configuration to which the present invention is applicable. The present invention is equally applicable to other user authentication mechanisms which utilize a remote authentication device and the exchange of any type of authenticated credential which could be saved for later use in authenticating a user as described herein.

[0015] In accordance with the present invention, and with reference to Figure 1, a user's computer system (referred to herein as a client or a client computer) 10 operates on a local area network (LAN) 20 or other type of local network. The local network also includes other computing devices, some of which house services or other resources which may be accessed from the client and which require user authentication before access is granted 30 (collectively referred to herein as secure resources). The client 10 may also itself house secure resources 30. The client 10 is also connected to a network providing more global access 40, such as a company-wide intranet or the worldwide communications network known as the internet. Through this global network, the client 10 is connected to a remote authentication server 60. The client may also access secure resources 30 located on the global network 40.

[0016] Connectivity from the client 10 to the global network 40 may optionally be provided through a secure gateway machine 50. The gateway machine 50 may connect several local clients (not shown) to the global network 40, centralizing the connections and providing a level of security between the clients, the LAN 20 and the global network 40.

[0017] With reference to Figure 2, when a user at the client attempts to access 100 a secure resource, whether locally or remotely, a user authentication is attempted 110 with an LDAP server. If the user authentication is successful 120, an authenticated credential is returned to the client by the authorization server 130. The authenticated credential is unique to the authenticated user and allows the client to access the requested secure resource 135.

[0018] When operating in accordance with the present invention, the authenticated credential is securely cached 140 on the client machine and, if one is present, on the gateway machine. In order to protect the credential from being tampered with or

falsified, the credential must be stored in a protected manner. This may be done using any one of the many methods known for such purposes to those skilled in the relevant arts. As an example, the credential may be protected by Public Key Infrastructure (PKI). The PKI standard provides for a method whereby the credential is encrypted before storing, preventing anyone from discovering its contents. PKI also provides the credential with a digital signature to detect whether the contents have been altered. The PKI method includes a Key which is stored on the client and which is used to encrypt and decrypt the credential. For an additional level of security, hardware-based PKI may be used wherein the Key is stored in hardware as opposed to the client's disk drive. This makes it much more difficult for a hacker to discover the Key. There are many other types of encryption and other security measures which may be applied to the stored credential, any of which may be used with the present invention. The various types of security measures available provide varying levels of security and require varying levels of complexity in implementing. The choice of a protection measure for a particular application is a selection to be made based on the level of sensitivity of the secure resources to be protected balanced against the available resources for implementation.

[0019] In accordance with the present invention, if a user authentication request fails 120, the client determines whether connectivity to an operative LDAP server is available 150. This determination may be performed using any method or technique known to those reasonable skill in the relevant arts. Such connectivity will not be available if the user authentication request failed because a connection between a client and the LDAP server is broken or because the LDAP server itself is down. If such connectivity is not available, the client checks the client machine for an authenticated credential matching the user whose authentication request failed 160. This search will necessarily involve decrypting the authenticated credential using whatever encryption method was used to protect the credential and verifying that the credential has not been tampered with. If a valid match is found 170, the user may access the requested resource using the locally stored credential 180. If no valid matching authenticated credential is found, the request to access the secure resource fails 190.

[0020] A system operating in accordance with the present invention may optionally implement system security policies limiting the use of local credentials for accessing

secure resources. For example, very sensitive resources may be defined by the system security policies as always requiring user authentication by an LDAP server. Less sensitive resources may require the last LDAP server authentication to have been received less than a certain number of hours prior to the current request. Still less sensitive resources might allow local credentials to be used without restriction. System security policies may be designed using any criteria known to those of reasonable skill in the art in order to appropriately protect the secure resources of varying levels of sensitivity.

[0021] Referring now to Figure 3 in a system including a secure gateway machine as described above, when a user authentication fails due to lack of connectivity to an operative LDAP server 150, the next step is to test for connectivity to an operative gateway machine 200. If such connectivity exists, the client checks the gateway 210 for an authenticated credential matching the user whose authentication request failed. Again, this search will necessarily involve decrypting the authenticated credential using whatever encryption method was used to protect the credential and verifying that the credential has not been tampered with. If a valid match is found 220, the user may access the requested resource using the authenticated credential found on the gateway 230. If no valid matching authenticated credential is found on the gateway 220, the request to access the secure resource fails 240.

[0022] The use of a gateway-stored credential is considered preferable to a credential stored on the client. The gateway machine is typically a secure machine utilizing network firewall software to isolate the gateway from unwanted intrusions from connected networks and is often maintained at a secure site. Also, since a gateway often provides connectivity to the global network for several (or many) clients, the likelihood of finding a matching authenticated credential is greater. Finally, in environments where users may use more than one network-attached workstation within the local network, all connecting to the global network through the gateway, once the user has been authenticated, the corresponding credential will reside on the gateway and the user may be authenticated at the gateway from any of the locally-networked workstations.

[0023] Again, a system operating in accordance with the present invention may optionally

implement system security policies selectively limiting access to sensitive resources using credentials not provided by the LDAP server. These limitations could also apply to gateway-stored credentials. Because gateways are typically more secure than clients, policies would typically allow access to more sensitive resources using gateway credentials than with locally-stored credentials. As stated above, system security policies can be designed by those reasonably skilled in the art as they feel appropriate under the circumstances.

[0024] If, when a user authentication request fails in a system including a gateway machine, no connectivity is available to an operative LDAP server or an operative gateway, the local client is searched 160 and a matching locally-stored authenticated credential used 180, if applicable, as discussed above.

[0025] In the situation where a user authentication request has failed but connectivity to an operative LDAP server *is* available 150, this indicates that a submitted user identification has been identified as not authorized to the requested resource. In accordance with the present invention a search is made of the client and the gateway, if applicable, for any earlier-authenticated credentials matching the user who has been denied authentication. Any matching credentials are flushed from the secure cache(s) 250 to ensure that user is not able to use the stored credentials to improperly access the secure resource(s). This situation could occur, if, for example, a user was authorized to a resource for a time but the authorization later expired or was revoked.

[0026] With respect to the functions and processes described and illustrated herein, each may be embodied in electronic circuitry (or hardware) or as a series of computer programming code instructions (or software) implementing the functions or steps described, or as a combination of hardware and software. For example, in this description and in the following claims where the client 10 (figure 1) is said to take some action or perform some function, that action or function may be effected by the execution of software in the memory (not shown) of client 10 as is well known by persons skilled in the relevant arts. Alternatively, such action or function may be effected by instructions implemented in the circuitry (not shown) of client 10, again, using techniques well known by those skilled in the relevant arts.

[0027] As readily recognized by those skilled in the art, the exact order of the steps

illustrated and discussed herein may be varied in any advantageous manner without deviating from the present invention. Also, where appropriate, steps may be repeated, skipped or combined to better operate in a given environment.

[0028] In the drawings and specification there has been set forth preferred embodiments of the invention, and, although specific terms are used, the description thus given uses terminology in a generic and descriptive sense only and not for purposes of limitation.